UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	M-11702 US	6041

32605 7590 09/24/2007

MACPHERSON KWOK CHEN & HEID LLP
2033 GATEWAY PLACE
SUITE 400
SAN JOSE, CA 95110

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
09/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/927,928	FAN ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6, 8-11, 15-17, 20, 25-27, 29-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 29, 2007 has been entered.

Claims 5, 7, 12-14, 18-19, 21-24, and 28 are cancelled.

Claims 1-4, 6, 8, 10-11, 16-17, 20, 26, and 29-32 are amended.

Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 are pending and herein considered.

Response to Arguments

Applicant's arguments, with respect to Droge's failure to teach or suggest "encrypting and transmitting a first session key" as included in Applicant's newly amended independent claims, have been fully considered and are persuasive. The 35 USC 102(e) rejection of claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of *Kaufman* and further in view of *Droge*.

Applicant's arguments with respect to the Examiner's use of multiple references have been fully considered but they are not persuasive. Insofar as the Examiner is familiar with the Lindemann decision, she notes that the Court in Lindemann was faced with a case in which the Examiner had failed to account for particular limitations entirely and it was in response to that failure that the court made it clear that each and every limitation of the claim must be taught by a reference. Although taken out of context Applicant's quotation seems to provide for the case at hand, the Examiner would like to point out that her inclusion of the Schneier reference was not intended to provide for limitations missing from the primary Droge reference, but rather to provide Applicant's representative with a reference disclosing those elements inherent to a DES system, elements that a person skilled in the art would understand to be included within the Droge reference simply by his mention of a DES system. Were it the Examiner's intention to supplement the Droge reference with Schneier, she would have amended her rejections in conformance with 35 USC 103(a). Insofar as that was not her intention, she maintains that her single reference 102(e) rejection of the claims was proper, and that her inclusion of the Schneier reference to disclose those elements inherent in the DES system of Droge was proper as well. Additional support for the Examiner's utilization of a reference in order to show characteristics inherent to but not disclosed in a primary reference may be found in section 2131.01 of the Manual of Patent Examining Procedure, namely section III entitled "To Show that a Characteristic Not Disclosed in the Reference is Inherent." Section 2131.01 provides citation to Continental Can Co. USA v. Monsanto Co wherein the court went on to explain that

"this modest flexibility in the rule that anticipation' requires that every element of the claims appear in a single reference accommodates situations in which the common knowledge of technologists is not recorded in the reference; that is, where technological facts are known to those in the field of the invention, albeit not known to judges." Continental Can Co. USA v. Monsanto Co., 948 F.2d 1264, 1268, 20USPQ2d 1746, 1749-50 (Fed. Cir. 1991)

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner is unsure how exactly "a first session uses a symmetric key" and what exactly the first session key is using it for. The Examiner is under the impression that the Applicant meant to claim "wherein the first session key is a symmetric key" and will treat the claim as such for purposes of furthering prosecution.

Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner is unsure how exactly "a second session key uses a symmetric session key" and what exactly the second session key is using it for. The Examiner is under the impression that the Applicant meant to claim "wherein the

second session key is a symmetric key" and will treat the claim as such for purposes of furthering prosecution.

Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 claims "a first session key" on two separate instances. The Examiner is under the impression that Applicant's second "a first session key" should have read "the first session key" and has chosen to treat it as such for purposes of furthering prosecution. As a result of the error, Applicant's subsequent reference to "the first session key" in claim 6 is also indefinite because it is unclear which "first session key" he is referring to.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 8 recites the limitation " the wireless device." There is insufficient antecedent basis for this limitation in the claim.

Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 9 recites the limitation " the first encryption algorithm." There is insufficient antecedent basis for this limitation in the claim.

Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 10 recites the limitation " forwards the decrypted encrypted payload and the header to the server" but at no point calls for the decryption

of the encrypted payload. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11 recites the limitation "decrypting the encrypted data packet at the gateway to recover *a decrypted data packet* comprising the encrypted payload encrypted with the first session key." It is unclear whether this "a decrypted data packet" is the same "a data packet" that was claimed in claim 10. The Examiner is under the impression that Applicant's "a decrypted data packet" should have read "the decrypted data packet" and has chosen to treat it as such for purposes of furthering prosecution.

Claim 30 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner is unsure how exactly "a first session uses a symmetric key" and what exactly the first session key is using it for. The Examiner is under the impression that the Applicant meant to claim "wherein the first session key is a symmetric key" and will treat the claim as such for purposes of furthering prosecution.

Claim 32 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner is unsure how exactly "the first session key uses a symmetric session key" and what exactly the first session key is using it for. The Examiner is under the impression that the Applicant meant to claim "wherein the first

session key is a symmetric key" and will treat the claim as such for purposes of furthering prosecution.

Claim 33 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 33 recites the limitation "wherein the first session key comprises at least one of the encryption algorithms DESX or DES." The Examiner is unacquainted with how a first session key could "comprise" an encryption algorithm.

Claim Objections

Claim 6 is objected to because of the following informalities: Applicant's placement of a semicolon between the words "network" and "comprising" in line 2 of the claim is improper. Appropriate correction is required.

Claim 32 is objected to because of the following informalities: Claim 32 is a duplicate of claim 30. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 5,081,678 to *Kaufman et al.*, and further in view of United States Patent Application Publication No. 2002/0004898 A1 to *Droge*.

As per **claim 1**, Kaufman teaches a method for transmitting secured data over a wireless link, the method comprising: encrypting a payload according to a first session key (col.3 lines 6-13); adding a header to the encrypted payload to form a data packet (col.4 lines 59-68); encrypting the first session key (col.3 lines 14-20); transmitting the encrypted first session key to a wireline device (col.3 lines 14-20); and transmitting the encrypted data packet over a wireless link to a gateway which recreates the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network (col.3 lines 21-33).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key and decrypting the encrypted data packet at gateway.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data

packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet.

As per **claim 2**, the combined method of Kaufman and Droge wherein the first session key uses a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 3**, the combined method of Kaufman and Droge teaches receiving the encrypted first session key and the encrypted payload at the wireline device (Kaufman col.3 lines 27-31); decrypting the encrypted first session key (Kaufman col.3 lines 27-31); and decrypting the encrypted payload using the decrypted first session key (Kaufman col.3 lines 27-31).

As per **claim 4**, the combined method of Kaufman and Droge teaches wherein the second session key uses a symmetric session key (col.3 lines 6-20).

As per **claim 6**, Kaufman teaches a device for transmitting data over a wireless link to a gateway providing access to a wide area network comprising: an encryption engine which generates a first session key (col.3 lines 6-13), encrypts a payload according to a first session key (col.3 lines 6-13), adds a header to the payload to form a data packet (col.4 lines 59-68), encrypts the first session key (col.3 lines 14-20); and a wireless transceiver coupled to the encryption engine which transmits the encrypted first session key (col.3 lines 14-20) and transmits the encrypted data packet over a

wireless link to a gateway which decrypts the encrypted data packet (col.3 lines 21-33), recreates the encrypted payload an the header (col.3 lines 21-33), and forwards the encrypted payload and the header to a server over an open network (col.3 lines 21-33).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key and decrypting the encrypted data packet at the gateway. Kaufman also fails to specifically disclose a wireless link to the gateway.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireline and wireless networks and links that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet as well as the wireless networks and links as described in Droge to provide for increased network flexibility.

As per **claim 8,** the combined method of Kaufman and Droge teaches wherein the payload comprises information regarding a location of the device (Kaufman col.4 lines 59-68).

As per **claim 9**, the combined method of Kaufman and Droge teaches wherein the first encryption algorithm employs a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 10**, Kaufman teaches a method for secured communication between a mobile device and a server on a wide area network, comprising: encrypting an unencrypted first session key at the mobile device (col.3 lines 14-20); transmitting the encrypted first session key to the server over a link (col.3 lines 14-20); decrypting the encrypted first session key at the server (col.3 lines 21-33); encrypting a payload at the device using the unencrypted first session key (col.3 lines 6-13); adding a header to the payload to form a data packet at the device (col.4 lines 59-68); encrypting the data packet according to a second session key configured for secured communications over the link; and transmitting the encrypted data packet from the device to a gateway which recreates the encrypted payload and the header, and forwards the decrypted encrypted payload and the header to the server (col.3 lines 21-33).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key and decrypting the encrypted data packet at the gateway. Kaufman also fails to specifically disclose the wireless capabilities provided for within the instant application including the wireless link and mobile device.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge

Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireless networks and mobile devices that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet as well as the wireless links and devices as described in Droge to provide for increased network flexibility.

As per **claim 11**, the combined method of Kaufman and Droge teaches receiving the encrypted data packet at the gateway (Kaufman col.3 lines 27-31); decrypting the encrypted data packet at the gateway to recover a decrypted data packet comprising the encrypted payload encrypted with the first session key (Droge paragraph 13); forwarding the decrypted data packet to the server over the wide area network (Droge paragraph 13); decrypting the encrypted first session key at the server using a private key (Kaufman col.3 lines 27-31); decrypting the encrypted payload at the server using the decrypted first session key (Kaufman col.3 lines 27-31).

As per **claim 15**, the combined method of Kaudman and Droge teaches wherein the payload includes location information (Kaufman col.4 lines 59-68).

As per **claim 16**, the combined method of Kaufman and Droge teaches wherein the generating a first session key at the mobile device further comprising generating the first session key based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 17,** the combined method of Kaufman and Droge teaches wherein the encrypting a payload using the first session key employs at least one of the encryption algorithms DESX or DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 20**, the combined method of Kaufman and Droge teaches wherein the first session key implements at least one of the encryption algorithms DESX or DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 25**, the combined method of Kaufman and Droge teaches wherein the data packet includes location information (Kaufman col.4 lines 59-68).

As per **claim 26**, the combined method of Kaufman and Droge teaches wherein the first session key is generated based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 27**, the combined device of Kaufman and Droge teaches a memory coupled to the encryption engine, the memory having a public key associated with a server on the wide are network stored therein (col.3 lines 6-20).

As per **claim 29**, Kaufman teaches a computer readable medium, comprising program instruction for performing a method comprising: encrypting a payload according to a first session key (col.3 lines 6-13); adding a header to the encrypted payload to form a data packet (col.4 lines 59-68); encrypting the first session key (col.3 lines 14-20); transmitting the encrypted first session key to a server (col.3 lines 14-20); and transmitting the data packet over a link to a gateway (col.3 lines 21-33) which recreates the encrypted payload and the header (col.3 lines 21-33), and forwards the encrypted payload and the header over an open network to the server which decrypts the encrypted first session key (Kaufman col.3 lines 27-31) and decrypts the encrypted payload using the decrypted first session key (Kaufman col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key configured for secured communications over a wireless link and decrypting the encrypted data packet. Kaufman also fails to provide for the use of wireless links and devices within his system.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also

discloses the use of both wireless networks and mobile devices that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet as well as the wireless links and devices as described in Droge to provide for increased network flexibility.

As per **claim 30**, the combined method of Kaufman and Droge teaches wherein the first session key using a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 31**, the combined method of Kaufman and Droge teaches receiving the data packet at the gateway (Kaufman col.3 lines 27-31); decrypting the data packet at the gateway according to the second session key (Droge paragraph 13); forwarding the encrypted payload to the server (Droge paragraph 13); receiving the encrypted first session key at the server (Kaufman col.3 lines 27-31); decrypting the encrypted first session key using a private key (Kaufman col.3 lines 27-31); and decrypting the payload according to the first session key (Kaufman col.3 lines 27-31).

As per **claim 32**, the combined method of Kaufman and Droge teaches wherein the first session key uses a symmetric session key (Kaufman col.3 lines 6-13).

As per claim 33, the combined method of Kaufman and Droge teaches wherein the first session key comprises at least one of the encryption algorithms DESX or DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 34**, the combined method of Kaufman and Droge teaches wherein the data packet includes location information (Kaufman col.4 lines 59-68).

As per **claim 35**, the combined method of Kaufman and Droge teaches wherein the symmetric session key is generated based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

T. Teslovich

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137